AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: s/Travis Leverett 9/18/2023

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with LAY.GREEN@ICLOUD.COM that is stored at premises controlled by Apple, Inc., a company headquarted at Apple, Inc., 1 Infinite Loop, Cupertino, California

Case No. M-23-813STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 846	Drug Conspiracy

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Cristina Busbee
Applicant's signature

Cristina Busbee, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: **Sep 18, 2023**

Shon T. Erwin
Judge's signature

City and state: Oklahoma City, Oklahoma

Shon T. Erwin, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH LAY.GREEN@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	Case No. MJ-23-813-STE **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Cristina Busbee, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since April 2019. I am presently assigned to the HSI office in Oklahoma City (hereinafter referred to as HSI Oklahoma City).

3. I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to

conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am authorized to conduct criminal investigations of violations of the laws of the United States and to execute warrants issued under the authority of the United States.

4. I have received approximately 26 weeks of specialized training at the Federal Law Enforcement Training Center in the enforcement of federal laws. I have arrested, interviewed, and debriefed numerous individuals who have been involved and have personal knowledge of transporting and concealing controlled substances and firearms, as well as, the amassing, spending, converting, transporting, distributing, laundering and concealing of proceeds from drug trafficking and smuggling. I have participated in numerous investigations involving physical and electronic surveillance. I have testified in judicial proceedings concerning the prosecution for violations of laws related to the illegal possession of firearms as well as the smuggling and trafficking of contraband, including controlled substances. I have been the affiant of numerous federal search warrants.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 846 have been committed by **Lamonn BLONNER** and other known and unknown persons. There is also

probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

7. HSI Oklahoma City is investigating a fentanyl smuggling organization operating in the Western District of Oklahoma and elsewhere. As part of this investigation, Lamonn **BLONNER** has been identified as a member of this drug trafficking organization responsible for taking substantial steps to further the organization's goals.

8. On July 17, 2023, law enforcement intercepted a shipment of approximately 21 kilograms of fentanyl-laced pills destined for Oklahoma City, Oklahoma. On July 19, 2023, a controlled delivery was conducted in Oklahoma City using an inert substance resembling the fentanyl pills. Law enforcement then monitored the controlled delivery of that inert substance to determine who would arrive to pick up the substance from the person law enforcement intercepted on July 17.

9. **BLONNER** was identified as the individual who arrived to retrieve the duffle bag containing the inert substance. **BLONNER** was driving a silver Chevy Malibu bearing Oklahoma license plate MDJ-359. Surveillance was conducted of **BLONNER** and he returned to his residence located at 209 NW 86th St., Oklahoma City, OK. Investigators observed **BLONNER** take the duffle bag inside the residence. Law enforcement knocked on the front door of the residence and **BLONNER** attempted to flee through the back window, at which point he was detained. Three minors and a female later identified as

Torquisha KESSEE were also at the residence. Investigators secured the residence and obtained a search warrant.

10. During the execution of the search warrant, investigators discovered a chamber loaded firearm in the Malibu that **BLONNER** was driving and three additional firearms inside the residence. Three of the firearms, including the firearm in **BLONNER's** vehicle were reported stolen. Additionally, investigators located 18 auto sears and a variety of controlled substances, including approximately 1.2 kilograms of cocaine, 240 grams of fentanyl pills, 280 grams of methamphetamine, and 760 grams of fentanyl powder.

11. On July 27, 2023, a federal search warrant was signed in the United States District Court for the Western District of Oklahoma for an Apple A2220 iPhone 11 Pro Max that was seized during the execution of the search warrant at 209 NW 86th St., Oklahoma City, OK. The phone was located on **BLONNER's** person at the time he was encountered. A forensic data extraction of the phone was conducted but was only partially successful. However, the extraction did reveal the Apple ID, lay.green@icloud.com, and phone number 405-978-9184[1].

12. I believe this Apple ID was used by **BLONNER** given it was identified through the phone that was on **BLONNER's** person at the time of his arrest. The phone's forensic extraction revealed that the user conducted Facebook searches for several other

[1] On August 22, 2023, HSI Oklahoma City served a subpoena to T-Mobile for subscriber information from of 6/1/2023 - 7/19/2023 for the phone number 405-978-9184. T-Mobile responded on the same day indicating there was no subscriber information available.

BLONNER's, including *Quint BLONNER, Dommanic Coolazz BLONNER, Kenyeah BLONNER, Malik BLONNER,* and *Marrcus BLONNER*, among others. The forensic extraction also revealed that the Apple ID is associated with the cellular devices Messages, iCloud, iTunes Store, IDMS, CloudKit, IMAPMail, Device Locator, Find My Friends, and Game Center.

13. On August 29, 2023, a preservation request was sent to Apple, Inc for the Apple ID: lay.green@icloud.com.

14. Based on my training, experience, and research, I know that the seized cellphone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and messenger, among others. Data associated with these capabilities are often saved within or backed up to the iCloud. For instance, photographs and text messages which may be on the phone may also be backed up to the iCloud, allowing law enforcement to recover the information the same as accessing the cellular device. Examining **BLONNER's** iCloud account would allow more evidence to be discovered that was not possible from the forensic extraction of the cellular device.

15. From my training and experience, I know that drug smuggling is a conspiratorial crime. Individuals who engage in these crimes typically do so in groups with the assistance of others. In fact, during a post-*Miranda* interview following his arrest, **BLONNER** admitted to working with others in connection with his illegal activity in this case. These criminals often use their cell phones to communicate with other members of

the criminal organization, as well as to take photographs of illicit activities. The Device also records the GPS location of the Device and other data which would reveal the travel and whereabouts of the Device, enabling law enforcement to be able to identify **BLONNER's** travels relating to the violations under investigation. Records of these communications, contact information of the conspirators and other data are often saved in a cloud-based system.

INFORMATION REGARDING APPLE ID AND iCLOUD[2]

16. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

17. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

---

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords,

credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

18. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

19. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

20. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

21. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

22. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer

service, including communications regarding a particular Apple device or service, and the repair history for a device.

23. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

24. The nature of this investigation has to do with drug smuggling, and the source of the drugs is unknown. However, based on my training and experience, I know that the transportation of drugs is a conspiratorial crime. Given what is necessary to arrange for

the movement of drugs, I believe that having access to **BLONNER's** iCloud account would be helpful to the investigation. This would indicate who **BLONNER** was communicating with, how the process of transporting the drugs was organized, and what kinds of contraband (if different from what was seized) was being transported. In my training and experience, evidence of who was using an iCloud account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. **BLONNER's** Apple iPhone was likely used to communicate with those who hired him.

25. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Having access to this information may allow investigators to understand who organized the transportation of 21 kilograms of sham fentanyl pills seized from **BLONNER** on July 19, 2023, and whether **BLONNER** is involved in the wider conspiracy, or was simply a courier in a one-time deal.

26. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled

the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

27. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

28. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. For example, a list of apps could reveal banking institutions used by the target and other money sending mechanisms such

as Venmo and PayPal. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

29. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrant.

32. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Cristina Busbee

Cristina Busbee
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on Sept. 18, 2023

Shon T. Erwin

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with lay.green@icloud.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within up to 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 21 U.S.C. § 846 (drug conspiracy) involving **Lamonn BLONNER** since January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The possession and distribution of controlled substances.

b. Compensation for the carrying out of illegal activities.

c. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

d. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

e. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

f. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

g. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.